Configure FlexConnect OEAP with Split Tunnelling

Contents

Introduction Prerequisites Requirements Components Used Overview Important Facts Configure Network Diagram Configurations WLAN configuration AP Configuration Verify

Introduction

This document describes how to configure an indoor Access Point (AP) as a FlexConnect Office Extend AP (OEAP) mode and how to enable split tunneling so that you can define what traffic must be switched locally at the home office and what traffic must be switched centrally at the Wireless LAN Controller (WLC).

Contributed by Tiago Antunes, Nicolas Darchis Cisco TAC Engineers.

Prerequisites

Requirements

There configuration on this document assumes that the WLC is already configured in a Demilitarized Zone (DMZ) with Network Address Translation (NAT) enabled and that the AP is able to join the WLC from the home office.

Components Used

The information in this document is based on these software and hardware versions:

- WLCs with version AireOS 8.10(130.0) Software.
- Wave1 APs: 1700/2700/3700.
- Wave2 APs: 1800/2800/3800/4800, and Catalyst 9100 series.

The information in this document was created from the devices in a specific lab environment.

The information in this document was created from the devices in a specific lab environment. All of

the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

An OEAP provides secure communications from a Cisco WLC to a Cisco AP at a remote location, in order to extend the corporate WLAN over the Internet to an employee's residence. The user's experience at the home office is exactly the same as it would be at the corporate office. Datagram Transport Layer Security (DTLS) encryption between the AP and the controller ensures that all communications have the highest level of security. Any indoor AP in FlexConnect mode can act as an OEAP.

Important Facts

- Cisco OEAPs are designed to work behind a router or other gateway device that uses NAT. NAT allows a device, such as a router, to act as an agent between the Internet (public) and a personal network (private), which enables an entire group of computers to be represented by a single IP address. There is no limit to the number of Cisco OEAPs that you can deploy behind a NAT device.
- All the supported indoor AP models with integrated antenna can be configured as an OEAP except the AP-700I, AP-700W, and AP802 series APs.
- All OEAPs must be in the same AP group, and that group must contain no more than 15 Wireless LANs. A controller with OEAPs in an AP group publishes only up to 15 WLANs to each connected OEAP because it reserves one WLAN for the personal Service Set Identifier (SSID).

Configure

Network Diagram



Configurations

WLAN configuration

Step 1. Create a WLAN to assign to the AP Group. You do not need to enable the FlexConnect Local Switching option for this WLAN.

ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT	COMMANDS HELP FEEDBACK
WLANs	WLANs > Edit 'FlexOEAP_TEST'	
WLANS WLANS	General Security QoS Policy-Mapping Advanced	
Advanced	MBO State	KTS based CAC Policy Enabled
	Off Channel Scanning Defer	Radius Client Profiling
	Scan Defer Priority 0 1 2 3 4 5 6 7	DHCP Profiling
		HTTP Profiling
	Scan Defer Time(msecs) 100	Local Client Profiling
	FlexConnect	DHCP Profiling
	FlexConnect Local Exabled	HTTP Profiling
	Switching 2 Chaoled	PMIP
	FlexConnect Local Auth 12 Enabled	PMIP Mobility Type
	Learn Client IP Address 2 🖾 Enabled	PMIP NAI Type Hexadecimal V
	Vian based Central Enabled	PMIP Profile None V
	Central DHCP Processing Enabled	PMIP Realm
	Override DNS Enabled	Universal AP Admin Support
	NAT-PAT Enabled	Universal AP Admin
	Central Assoc Enabled	11v BSS Transition Support

Step 2. Create an AP group. On the **WLANs** tab, choose the WLAN SSID and then click **Add** to add the WLAN. Go to the **APs** tab and **Add** the FlexConnect OEAP.

،،ا،،،ا،، cısco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	Ap Groups > Edit 'FlexOEAP_Group'
VLANs	General WLANS RF Profile APS 802.11u Location Ports/Module Intelligent Capture
Advanced	Add New
	Add New WLAN SSID FlexOEAP_TEST(17)
	Interface /Interface management V 1 Group(G)
	SNMP NAC State
	WLAN ID WLAN SSID ^{(2)(g)} Interface/Interface Group(G) SNMP NAC State
ululu cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
WLANs	Ap Groups > Edit 'FlexOEAP_Group'
VLANS	General WLANS RF Profile APS 802.11u Location Ports/Module Intelligent Capture

 Advanced AP Groups 	APs currently in the Gr	oup	Remove APs	Add APs to the Group		Add APs
	AP Name	Ethernet MAC		AP Name	Group Name	
	AP9120_4C.E77C	c4:f7:d5:4c:e7:7c				
	AP3800_E1.3EB8	70:db:98:e1:3e:b8				

AP Configuration

After the AP has associated with the controller in FlexConnect mode, you can configure it as an

OEAP.

Step 1. After the AP joins the WLC, change the AP mode to **FlexConnect** and click **Apply**.

cisco	MONITOR WLANS	CONTROLLER WIRELESS	SECURITY MANAGEMENT	C <u>o</u> mmands hei	P FEEDBACK	
Wireless Access Points All APs	All APs > Details for	or AP3800_E1.3EB8	Availability Inventory	Advanced	Intelligent Capture	
Direct APs Radios 802.11a/n/ac/ax	General		Versions			
802.11b/g/n/ax Dual-SG Radios Dual-SG Radios Global Configuration Advanced Mesh AP Group NTP ATF RF Profiles FlexConnect Groups FlexConnect ACLs	AP Name Location AP MAC Address Base Radio MAC Admin Status AP Mode AP Sub Mode Operational Status Port Number Venue Group Venue Type	AP3800_E1.3E88 default location 70:db:98:e1:3e:b8 00:27:e3:36:5a:60 Enable local local local FlexConnect monitor Bridge FlexHerdge SE-Connect Unspecified	Primary Backup : Predown Predown Predown Predown Boot Ver IOS Ver Mini IOS IP Config CAPWAP	Software Version Software Version Iload Status Iloaded Version Iload Next Retry Tim Iload Retry Count rsion Sion S Version Preferred Mode	8.10.130.0 8.10.120.0 None None NA NA 1.1.2.4 8.10.130.0 0.0.0 Ipv4 (Global Config)	
Templates Network Lists 802.11a/n/ac/ax	Add New Venue Language Name Network Spectrum Interface Key	3D1781A0FFFC6B2F174A6EF605	DHCP Ip Static IP FB1DF8 Fabric	vv4 Address (Ipv4/Ipv6)	192.168.100.12	

Step 2. Make sure you have at least a Primary WLC configured in the High Availability tab:

cisco		CONTROLLER WIREL	ess security ma	NAGEMENT C	QMMANDS HELF	EEEDBACK			
Wireless	All APs > Details fo	or AP9120_4C.E770							
Access Points All APs	General Creder	tials Interfaces	High Availability	Inventory	FlexConnect	Advanced	Intelligent Capture		
Radios Roo Alaciadore		Name	Ма	Management IP Address(Ipv4/Ipv6)					
802.11b/g/n/ax 802.11b/g/n/ax	Primary Controller	19	2.168.1.14						
Dual-SG Radios Global Configuration	Secondary Controller		1						
Advanced									
Mesh	AP Failover Priority	Low ¥					1		
AP Group NTP									
ATF									
RF Profiles									
FlexConnect Groups									
FlexConnect ACLs									
FlexConnect VLAN Templates									
Natwork Lists									

Step 3. Go to the FlexConnect tab and check the Enable OfficeExtend AP check box.

	ာါကျက cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
W	ïreless	All APs > Details for AP3800_E1.3EB8
Ŧ	Access Points All APs	General Credentials Interfaces High Availability Inventory FlexConnect Advanced Intelligent Capture
	 Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios 	VLAN Support Make VLAN AP Specific V Go
	Dual-SG Radios Global Configuration	Inheritance Group-Specific
÷	Advanced Mesh	FlexConnect default-flex-group default-flex-group
Þ	AP Group NTP	WILAN AVC Mapping
÷	ATF	VLAN Template Name none
	RF Profiles	VLAN Name Id Mappings
	FlexConnect Groups	
÷	FlexConnect ACLs	PreAuthentication Access Control Lists
	FlexConnect VLAN Templates	External WebAuthentication ACLs
	Network Lists	Costal 2017 Acad
×	802.11a/n/ac/ax	
•	802.11b/g/n/ax	
Þ	Media Stream	OfficeExtend AP
÷	Application Visibility And Control	Enable OfficeExtend AP
	Lync Server	Enable Least Latency Controller Join
	Country	Reset Personal SSID
	Timers	Tunnel Gateway List
	Netflow	
	005	Total

DTLS **Data Encryption** is enabled automatically when you enable the OfficeExtend mode for an AP. However, you can enable or disable DTLS data encryption for a specific AP. To do so, check (enable) or uncheck (disable) the **Data Encryption** check box on the All APs > Details for [selected AP] > Advanced tab:

	ဂျကျက cisco	MONITOR 1	<u>w</u> lans <u>c</u> ontro	DLLER WIRELE	:SS <u>s</u> ecurity	MANAGEMENT	C <u>O</u> MMANDS	HELP E	EEEDBACK				
W	ireless	All APs > D	etails for AP9	120_4C.E77C				-	_				
*	Access Points All APs	General	Credentials	Interfaces	High Availabi	ity Inventory	FlexConn	ect A	dvanced	Network Diagno	stics	Intelligent Capture	
	Direct APs Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios Dual-SG Radios Global Configuration	Regulator Country (Cisco Dis AP Group	ry Domains Code covery Protocol Name		802.1 US (U S (FlexO	802.11bg:-A 802.11a:-B US (United States) ♥ ♥ FlexOEAP_Group ♥			Power Over Ethernet Settings PoE Status Pre-standard 802.3af switches Power Injector State				
	Advanced	Statistics	Timer		30				AP Core Dun	ıp	_		
	Mesh	Data Enc	ryption					-	AP Core Dump			lad	
•	AP Group NTP	Rogue De	tection						AP Retransmit Config Parameters				
	ATF	² Telnet			Globa	Config 🗸 🗌		-					
	RF Profiles	2 SSH			AP Sp	ecific 🖌 🗌			AP Retrans	smit Count	5	1	
	FlexConnect Groups	NSI Ports	State		Globa	l Config 💙 🖾			AP Retransmit Interval 3				
•	FlexConnect ACLs	TCP Adju	st MSS (IPv4: 536	- 1363, IPv6: 1220	0 - 1331) 🖾 🚺	250 MSS is Globally Ena	abled	v	VLAN Taggin	ino.	E E Dal	blad	
	FlexConnect VLAN Templates	LED State				able 💙		N	NTP Server Status				
	Network Lists	LED Brigh	tlevel		8	(1-8)			Status D	visabled			
Þ	802.11a/n/ac/ax	LED Flash	State		0	(1-3600)seco	onds	т	TrustSec				
	802.11b/g/n/ax					finite		-	TrustSec C	onfin			
•	Media Stream				Olisa	ble			MX Service	e			
	Application Visibility	USB Modu	ile ID		USB M	USB Module				-			
•	And Control	Override							Services S	ub-Services CMX S	erver Ip	<u> </u>	
	Lync Server	USB Modu	le Status		12								

Note: Telnet and SSH access are disabled automatically when you enable the OfficeExtend mode for an AP. However, you can enable or disable Telnet or SSH access for a specific AP. To do so, check (enable) or uncheck (disable) the Telnet or SSH check box on the All APs > Details for [selected AP] > Advanced tab.

Note: Link latency is enabled automatically when you enable the OfficeExtend mode for an AP. However, you can enable or disable link latency for a specific AP. To do so, check (enable) or uncheck (disable) the Enable Link Latency check box on the All APs > Details for [selected AP] > Advanced tab.

Step 3. Select **Apply**. After you select Apply, the AP reloads.

Step 4. After the AP rejoins the WLC, the AP is in OEAP mode.

Note: We recommend that you configure AP join security (commonly defined under AP Policies) so that only authorized APs can join the WLC. You can also use Locally Significant Certificate (LSC) AP provisioning.

Step 5. Create a FlexConnect Access Control List (ACL) to define which traffic will be switched centrally (Deny) and locally (Permit).

Here, you have the goal of switching locally all traffic to the subnet 192.168.1.0/24.

	ululu cisco	MONITOR WLANS CON	TROLLER	WIRELESS SECURI	Y HAVAGEMENT	COMMANDS HEL	P EEEDBACK					
Wireless * Access Points All APs Direct APs * Radios 802.11abn/ac/ax	FlexConnect ACLs > I General Access List Nerre	Pv4 ACL >	Edit									
,	Dual-Band Radios Dual-3G Radios Global Configuration Advanced	IP Rules Seq 1	Action	Source IP/Hask 0.0.0.0 / 0.0.0.0		Destination IP/I 192.168.1.0	Destination IP/Hask 192.168.1.0 / 255.255.255.0		Protocol Source Port		DSCP	
•	Mesh AP Group NTP ATF	2	Deny	0.0.0.0	/ 0.0.0.0	0.0.0.0	/ 0.0.0.0	Any	Any	Any	Any	_
C	RF Profiles FlexConnect Groups FlexConnect ACLS Jivis ACL Ilvis ACL FlexConnect VLAN Templates	URL Rules Seq Action		Destination Ur								

Step 6. Create a FlexConnect Group, go to **ACL Mapping**, and then go to **WLAN-ACL Mapping**. Under "Local Split ACL Mapping," enter the WLAN ID and choose the FlexConnect ACL. Then click **Add**.

cisco	MONITOR WLANS CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP EEEDBACK
Wireless	FlexConnect Groups > Edit 'FlexConnect_OEAP_Group'
 Access Points All APs 	General Local Authentication Image Upgrade ACL Mapping Central DHCP WLAN VLAN mapping WLAN AVC mapping
Direct APs • Radios 802.11a/n/ac/ax 802.11b/g/n/ax Dual-Band Radios Dual-SG Radios	AAA VLAN-ACL mapping WLAN-ACL mapping Policies
Global Configuration	Web Auth ACL Mapping
Advanced	WLAN Id 0
AP Group NTP	WebAuth IPV4 ACL none V Local Spit ACL Flex_OEAP_ACL V
ATF	WebAuth Dvb ACL none V
RF Profiles	WLAN Id WLAN Profile Name LocalSplit ACL
FlexConnect Groups	WLAN WLAN Profile WebAuth IPV4 WebAuth IPV6 17 FlexOEAP_TEST Flex_OEAP_ACL V
FlexConnect ACLs	
FlexConnect VLAN Templates	
Network Lists	
802.11a/n/ac/ax	

Step 7. Add the AP to the FlexConnect group:

cisco	MONITOR WLANS CO	WITROLLER WIRELESS S	ECURITY MANAGEMENT COMMANDS	HELP LEEDEN	«ск						
Wireless	FlexConnect Groups	> Edit 'FlexConnect_	OEAP_Group'								
Access Points All APs Direct APs * Radios 802.11a/n/sc/ax	General Local Aut	thentication Image Up	grade ACL Mapping Central Di	ICP WLAN VL	AN mopping WLAN AVC	mapping					
802-11b/g/n/ax Dual-Band Radios Dual-SG Radios Gibbal Conferention	VLAN Template Name Enable AP Local Authent	fication ²									
Advanced Mesh AP Group NTP	Electonnect AP	cisco	MONITOR WLANS CONTROLLER	WIRELESS SEC	urity management co	MMANDS HELP EEEDBAC	×				
> ATF	Ip Address(Ipv4/Ipv6)	Wireless	FlexConnect Group AP List								
RF Profiles FlexConnect Groups * FlexConnect ACLs	Port	Access Points All APs Direct APs V Radios	Group Name	RexConnect_	OEAP_Group						
IPv4 ACL IPv6 ACL ElexConnect VI AN	***	802.11a/n/ac/ax 802.11b/g/e/ax Dual-Bend Radios	FlexConnect APs		cisco	MONITOR WLANS CO	TROLLER WIRELESS SECURIT	у маладемент сомн	ANDS HELP ETEDBACK		
Templates Network Lists > 802.11a/n/ac/ax > 802.11b/g/n/ax	Server Ip Address Server Type Shared Secret Confirm Shared Secret	Dual-3G Radios Global Configuration Advanced Nesh AD Group NTP	Add AP Selett APa from carrent controller AP Name (AP3000 E1.5088 V) Nome (AP3120, eC.677C)	Wireless * Access Points Al APs Direct APs * Endice	FlexConnect Group A	P List RexCorne	ct_OEAP_Group			
Hedia Stream Application Visibility And Control	Port Number Add	ATF RF Profiles		dd Cancel	802.13a/n/ac/ax 802.13b/g/n/ax Dual-Band Radios Dual-5G Radios	ElexConnect APs					
Lync Server Country	4	FlexConnect Groups FlexConnect ACLs IPvd ACL IPvd ACL FlexConnect VLAN Templates	Entries 0 - 0 of 0 AP MAC Address AP Name	Status	Global Configuration Advanced Hesh AP Group NTP ATF	Add AP Select Afte from current of Ethernet HAC	Add Cancel				
		Network Lists			RF Profiles FlexConnect Groups * FlexConnect ACLs IPv6 ACL IPv6 ACL	Entries 1 - 2 of AP HAC Address 701db:98(e1:3e:b8 04:07:d5(4c:e7)7c	2 AP Name AP3000_E1.3688 AP9120_4C.677C	Status Associated Associated	AP Hode Rexistence Rexistence	Type Manual Manual	Conflict with PaP No Conflict No Conflict
					FlexConnect VLAN Templates						

Verify

1. Verify the FlexConnect ACL status and definition:

flexconnect nat-pat Flag..... Disabled flexconnect Dns Override Flag..... Disabled flexconnect PPPoE pass-through..... Disabled

c3504-01) >show flexconnect acl summary ACL Name Status ----- -----Flex_OEAP_ACL Applied (c3504-01) >show flexconnect acl detailed Flex_OEAP_ACL Source Destination Source Port Dest Port Index IP Address/Netmask IP Address/Netmask Prot Range Range DSCP Action _____ _____ --- ---- ------1 0.0.0.0/0.0.0.0 192.168.1.0/255.255.255.0 Any 0-65535 0-65535 Any Permit 2 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0 Any 0-65535 0-65535 Any Deny Verify that FlexConnect local switching is disabled: (c3504-01) >show wlan 17 WLAN Identifier..... 17 Profile Name..... FlexOEAP_TEST Network Name (SSID)..... FlexOEAP_TEST Status..... Enabled . . . Interface..... management . . . FlexConnect Local Switching..... Disabled FlexConnect Central Association..... Disabled flexconnect Central Dhcp Flag..... Disabled

flexconnect local-switching IP-source-guar... Disabled FlexConnect Vlan based Central Switching Disabled FlexConnect Local Authentication..... Disabled FlexConnect Learn IP Address..... Enabled Flexconnect Post-Auth IPv4 ACL..... Unconfigured Flexconnect Post-Auth IPv6 ACL.... Unconfigured ... Split Tunnel Configuration Split Tunnel.... Disabled Call Snooping..... Disabled Roamed Call Re-Anchor Policy.... Disabled ...

3. Verify the FlexConnect Group configuration:

(c3504-01) > show flexconnect group summary

FlexConnect Group Summary: Count: 2 Group Name # Aps

FlexConnect_OEAP_Group 2
default-flex-group 0

(c3504-01) >show flexconnect group detail FlexConnect_OEAP_Group

Number of AP's in Group: 2

```
AP Ethernet MAC Name Status Mode Type Conflict with PnP
```

70:db:98:e1:3e:b8 AP3800_E1.3EB8 Joined Flexconnect Manual No c4:f7:d5:4c:e7:7c AP9120_4C.E77C Joined Flexconnect Manual No

Efficient AP Image Upgrade Disabled

Efficient AP Image Join Disabled

Auto ApType Conversion..... Disabled

Master-AP-Mac Master-AP-Name Model Manual

Group Radius Servers Settings: Type Server Address Port

Primary Unconfigured Unconfigured Secondary Unconfigured Unconfigured

Group Radius AP Settings: AP RADIUS server.....

AP RADIUS server	Disabled
EAP-FAST Auth	Disabled
LEAP Auth	Disabled
EAP-TLS Auth	Disabled
EAP-TLS CERT Download	Disabled
PEAP Auth	Disabled
Server Key Auto Generated	No
Server Key	<hidden></hidden>
Authority ID	436973636f00000000000000000000000

Authority Info..... Cisco A_ID PAC Timeout..... 0 HTTP-Proxy Ip Address..... HTTP-Proxy Port..... 0 Multicast on Overridden interface config: Disabled DHCP Broadcast Overridden interface config: Disabled Number of User's in Group: 0 FlexConnect Vlan-name to Id Template name: none Group-Specific FlexConnect Local-Split ACLs : WLAN ID SSID ACL ----- ----- -----17 FlexOEAP_TEST Flex_OEAP_ACL Group-Specific Vlan Config: Vlan Mode..... Enabled Native Vlan..... 100 Override AP Config..... Disabled Group-Specific FlexConnect Wlan-Vlan Mapping:

WLAN TO Vlan TD

WLAN ID SSID Central-Dhcp Dns-Override Nat-Pat

You can capture the traffic at the AP interface in order to verify that the traffic is split at the AP.

Tip: For troubleshooting purposes, you can disable DTLS encryption in order to see the data traffic encapsulated inside capwap.

This packet capture example shows data traffic that matches the ACL "deny" statements directed to the WLC, and data traffic that matches the ACL "permit" statements switched locally at the AP:

Ethernet_yellowCable											
File	Edit View Go	Capture	Analyze Statistics Telephony	Wireless Tools Help							
1	🗖 🧕 🕘 🗍 🗄	NO C	९ 🕫 🕫 🗑 🛓 📃 📃	Q, Q, Q, II							
II ia	mp										
No.	Delta	1	Source	Destination	Length	Info		Ext Tag Number			
+	28859	9.819533 1	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	158	Echo (ping) request	id=0x0001, seq=213/545_				
e	20860	0.019956 1	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo (ping) reply	id=0x0001, seq=213/545_				
	20912	0.984274	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo (ping) request	id=0x0001, seq=214/547_				
	20913	0.018616 1	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo (ping) reply	id=0x0001, seq=214/547_				
	20961	0.986005 1	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo (ping) request	id=0x0001, seq=215/550_				
	20962	0.018343 1	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo (ping) reply	id=0x0001, seq=215/550_				
	21007	0.984777 1	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo (ping) request	id=0x0001, seq=216/552_				
	21008	0.018309 1	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	t Echo (ping) reply	id=0x0001, seq=216/552_				
	21467	9.477613 1	192.168.1.99	192.168.1.254	74	Echo (ping) request	id=0x0001, seq=217/555_				
	21468	0.000638	192.168.1.254	192.168.1.99	74	Echo (ping) reply	id=0x0001, seq=217/555_				
	21511	1.003331 1	192.168.1.99	192.168.1.254	74	Echo (ping) request	id=0x0001, seq=218/558_				
	21512	0.000192 1	192.168.1.254	192.168.1.99	74	Echo (ping) reply	id=0x0001, seq=218/558_				
	21572	1.009272 1	192.168.1.99	192.168.1.254	74	Echo (ping) request	id=0x0001, seq=219/560_				
	21573	0.000000 1	192.168.1.254	192.168.1.99	74	Echo (ping) reply	id=0x0001, seq=219/560_				
	21621	1.002280 1	192.168.1.99	192.168.1.254	74	Echo (ping) request	id=0x0001, seq=220/563_				
	21622	0.000374 1	192.168.1.254	192.168.1.99	74	Echo (ping) reply	id=0x0001, seq=220/563_				

> Frame 20859: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0

Ethernet II, Src: Cisco_e1:3e:b8 (70:db:98:e1:3e:b8), Dst: Cisco_14:04:b0 (cc:70:ed:14:04:b0)

Internet Protocol Version 4, Src: 192.168.1.99, Dst: 192.168.1.14

> Internet Protocol Version 4, Src: 192.168.1.139, Dst: 8.8.8.8 > Internet Control Message Protocol

User Datagram Protocol, Src Port: 5264, Dst Port: 5247

> Control And Provisioning of Wireless Access Points - Data > IEEE 802.11 Data, Flags:T

> Logical-Link Control

4	C *Ethernet_yellowCable										
File	Edit View Go	Capture	Analyze Statistics Telephony	Wireless Tools Help							
Æ.	📕 🔬 🛞 🛄 🛅	XC	۹ 👄 🗢 🕾 Ŧ 🛓 🚍 🔳	Q, Q, Q, II							
I komp											
No.	Delta		Source	Destination	Length	Info					Ext Tag Numb
1	28859	9.819533	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo	(ping)	request	id=0x0001,	seq=213/545_	
	28868	0.019956	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=213/545_	
	20912	0.984274	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo	(ping)	request	id=0x0001,	seq=214/547_	
	20913	0.018616	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=214/547_	
	20961	0.986005	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo	(ping)	request	id=0x0001,	seq=215/550_	
	28962	0.018343	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=215/550_	
	21007	0.984777	192.168.1.99,192.168.1.139	192.168.1.14,8.8.8.8	150	Echo	(ping)	request	id=0x0001,	seq=216/552_	
	21008	0.018309	192.168.1.14,8.8.8.8	192.168.1.99,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=216/552_	
+	21467	9.477613	192.168.1.99	192.168.1.254	74	Echo	(ping)	request	id=0x0001,	seq=217/555_	
+	21468	0.000638	192.168.1.254	192.168.1.99	74	Echo	(ping)	reply	id=0x0001,	seq=217/555_	
	21511	1.003331	192.168.1.99	192.168.1.254	74	Echo	(ping)	request	id=0x0001,	seq=218/558	
	21512	0.000192	192.168.1.254	192.168.1.99	74	Echo	(ping)	reply	id=0x0001,	seq=218/558_	
	21572	1.009272	192.168.1.99	192.168.1.254	74	Echo	(ping)	request	id=0x0001,	seq=219/560_	
	21573	0.000000	192.168.1.254	192.168.1.99	74	Echo	(ping)	reply	id=0x0001,	seq=219/560_	
	21621	1.002280	192.168.1.99	192.168.1.254	74	Echo	(ping)	request	id=0x0001,	seq=220/563_	
L	21622	0.000374	192.168.1.254	192.168.1.99	74	Echo	(ping)	reply	id=0x0001,	seq=228/563_	

> Frame 21467: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0

> Ethernet II, Src: Cisco_e1:3e:b8 (70:db:98:e1:3e:b8), Dst: ThomsonT_73:c5:1d (00:26:44:73:c5:1d)

> Internet Protocol Version 4, Src: 192.168.1.99, Dst: 192.168.1.254

> Internet Control Message Protocol

Note: In normal scenarios, the AP translates network addresses for locally switched traffic because the client subnet belongs to the office network, and local devices at the home office do not know how to reach the client subnet. The AP uses the IP address that is defined in the local home office subnet to translate the client traffic.

In order to verify that the AP performed the NAT, you can connect to the AP terminal and issue the "*show ip nat translations*" command. Example:

AP3800_E1.3EB8#show ip nat translations

TCP NAT upstream translations: (192.168.1.139, 1223, 192.168.1.2, 5000) => (192.168.1.99, 1223, 192.168.1.2, 5000) [*0 gw_h/nat/from_inet_tcp:0] i0 exp42949165 (192.168.1.139, 1095, 192.168.1.2, 5000) => (192.168.1.99, 1095, 192.168.1.2, 5000) [*0 gw_h/nat/from_inet_tcp:0] i0 exp85699 ... TCP NAT downstream translations:

(192.168.1.2, 5000, 192.168.1.99, 1223) => (192.168.1.2, 5000, 192.168.1.139, 1223)
[gw_h/nat/to_inet_tcp:0 *0] i0 exp42949165
(192.168.1.2, 5000, 192.168.1.99, 1207) => (192.168.1.2, 5000, 192.168.1.139, 1207)
[gw_h/nat/to_inet_tcp:0 *0] i0 exp85654

If you remove split tunneling, then all traffic is switched centrally at the WLC. This example shows the Internet Control Message Protocol (ICMP) to the 192.168.1.2 destination, inside the capwap tunnel:

File E	dit View G	o Capture	Analyze Statistics Telephony V Q @ @ @ 2 1 2 2 2 0 0	Vireless Tools Help Q Q III						
kmpl										
No.	Delta	P	Source	Destination	Length	Info				
	108	0.000000	192.168.1.82,192.168.1.139	192.168.1.14,192.168.1.2	150	Echo	(ping)	request	id=0x0001,	seq=129/330
-	109	0.000046	192.168.1.14,192.168.1.2	192.168.1.82,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=129/330
	127	1.000716	192.168.1.82,192.168.1.139	192.168.1.14,192.168.1.2	150	Echo	(ping)	request	id=0x0001,	seq=130/332
	128	0.000266	192.168.1.14,192.168.1.2	192.168.1.82,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=130/332
	142	1.005703	192.168.1.82,192.168.1.139	192.168.1.14,192.168.1.2	150	Echo	(ping)	request	id=0x0001,	seq=131/335
	143	0.000130	192.168.1.14,192.168.1.2	192.168.1.82,192.168.1.139	142	Echo	(ping)	reply	id=0x0001,	seq=131/335
	165	1.008894	192.168.1.82,192.168.1.139	192.168.1.14,192.168.1.2	150	Echo	(ping)	request	id=0x0001,	seq=132/337
	166	0.000133	192,168,1,14,192,168,1,2	192,168,1,82,192,168,1,139	142	Echo	(ning)	reply	id=0x0001.	seg=132/337

Ext Tag Number

Payload Type

MSDU MSDU MSDU MSDU MSDU

MSDU MSDU

MSDU

Ch

> Frame 108: 150 bytes on wire (1200 bits), 150 bytes captured (1200 bits) on interface 0
> Ethernet II, Src: Cisco_4c:e7:7c (c4:f7:d5:4c:e7:7c), Dst: Cisco_14:04:b0 (cc:70:ed:14:04:b0)
> Internet Protocol Version 4, Src: 192.168.1.82, Dst: 192.168.1.14
> User Datagram Protocol, Src Port: 5251, Dst Port: 5247
> Control And Provisioning of Wireless Access Points - Data
> IEEE 802.11 Data, Flags:T
> Logical-Link Control
> Internet Protocol Version 4, Src: 192.168.1.139, Dst: 192.168.1.2
> Internet Control Message Protocol